# 1 Introduction

In the global research environment, researchers ofter travel to other institutions for meeting and research collaboration. One of the essential service required by all researcher is access to the Internet. One option, an expansive option, is to subscribe to roaming data plans offered by telco. However, this is expansive and furthermore most research institution have Internet access, it is just the visitors need to get the account.

eduroam[xxx] is an international secure roaming service implemented for the research and education communities to address the issue of providing seamless Internet access to visiting academic/researchers to the institution. It is currently implemented in 74 countries from North and South America, Europe and Asia. eduroam provides users from participating institutes seamless and secure wifi access to the Internet at other participating institutions around the world.

Eduroam utilises a hierarchical RADIUS server infrastructure and the IEEE 802.1x standard networking protocol to provide roaming Internet service across research and education networks across the world. (GEANT Association, 2014) The RADIUS server hierarchy is involved in forwarding user credentials to the home institution of the user for validation and verification purposes. The IEEE 802.1x technology standard[xxx] defines the end-to-end encryption and authentication protocol over the wireless connection offered by Eduroam.

Host institution is th institution that is providing the access point.

Home institution is the institution the visiting research reside.

Authentication and authorisation of access is performed under the following arrangement, where users are authenticated at their home institutions which act as Identity Providers (IdPs) and the authorisation for user network access is handled by the Service Providers (SPs) providing the access points. When the user first requests authentication at a SP, the SP looks for the realm of the user that indicates the IdP associated with the user. The realm can be found in the form of userid@IdP.TLD, where IdP refers to the domain name of the home institution and TLD indicates the top-level domain of the home institution belongs.(Could you give an example ) Each institution has its own RADIUS server connected to a local user database. With the information from the user realm, the RADIUS server can route that request to the following suitable RADIUS server until the correct Identity Provider is reached. At the Identity Provider, the user authentication details can be validated with the user data in the local database and transport the validation result back to the SP. User access authorisation is then conducted by the SP and network access is granted to the user by allocating a specific VLAN for visitors.

The secure transmission of user authentication details across the RADIUS server infrastructure is maintained by the IEEE 802.1x standard, which utilises the Extensible Authentication Protocol (EAP). The function of EAP is to encapsulate the authentication data such that only the user and its IDP are aware of the actual authentication process, and other users will be unable to hijack the connection after successful verification. WPA2-Enterprise, a security mechanism for wireless networks, is used for encrypting the authentication data to prevent eavesdropping for the user credentials.

**Organisation of Eduroam Infrastructure**

The following diagram is an illustration of the hierarchical RADIUS server infrastructure adopted by Eduroam. It is divided into 3 levels, namely the Confederation level(ETLRs), the Federation level(FLRs) and lastly, the Institutional level(IdPs and SPs). (M. Milinović, 2012)

The confederation top-level RADIUS (TLR) servers are authoritative top-level domains coordinating the operation of eduroam servers within the regions under their jurisdiction. Each TLR has a list of connected country domains serving the appropriate National Research and Education Networks(NRENs). The TLRs accept requests for federation domains under their authority and then forward them to the respective federation RADIUS server. Requests for domains not under their authority would be forwarded to the proper confederation server. Currently, there are two confederation-level TLRs based in Europe known as ETLRs that handle requests from the European NRENs and also NRENs from other parts of the world.

Figure 1a: Hierarchical representation of Eduroam servers

The federation-level RADIUS (FLR) servers are responsible for handling requests between the IDPs/SPs and the upstream confederation TLRs. Each FLR possess a list of connected IdPs and SPs, and they redirect requests to the proper SP based on the user realm. Requests with destinations not under their authority would be forwarded upstream to the TLR. The FLR is operated by the NREN of the territory to manage connections from its member institutes. For instance, the FLR for Singapore is maintained by SingAren. (Singapore Advanced Research & Education Networks, 2014)

The bottom-level servers consist of IdPs and SPs participating in eduroam. They are responsible for the actual authentication of their own users through the validation of the user’s credentials with their internal database. They are also tasked with forwarding access requests from visiting users to the associated federation server.

The hierarchical structure of RADIUS servers hence ensures that the transport of user authentication details can be conducted effectively between the SPs and the IdPs across different federations of networks.

# Bibliography

GEANT Association. (2014, August 12). *eduroam in a nutshell*. Retrieved from https://wiki.geant.org/display/H2eduroam/eduroam+in+a+nutshell

M. Milinović, S. /. (2012, July 26). *eduroam Policy Service Definition*. Retrieved from https://www.eduroam.org/downloads/docs/GN3-12-192\_eduroam-policy-service-definition\_ver28\_26072012.pdf

Singapore Advanced Research & Education Networks. (2014, July 31). *eduroam Project - Welcome to eduroam in Singapore*. Retrieved from SingAren Web Site: http://www.singaren.net.sg/Eduroam.php